Information Commissioner's Office
Internal Audit Plan 2017-18

May 2017

Contents

It is the responsibility of Information Commissioners Office's management to ensure that there are adequate risk management, governance and control arrangements.

1 Developing the Internal Audit Plan

1.1 Overview of our internal audit approach

Our role as internal auditor to an executive NDPB is to provide an independent and objective opinion to the Management Board on the adequacy and effectiveness of its risk management, control and governance processes. Our approach, as set out in the firm's Internal Audit Manual, is to help the organisation to accomplish its objectives by bringing a systematic, disciplined approach to our evaluation and to help improve the effectiveness of its risk management, control and governance processes.

Our approach complies with best professional practice, in particular, the standards for internal audit promulgated by HM Treasury (Public Sector Internal Audit Standards, PSIAS), and the Institute of Internal Auditors' guidance on risk-based internal auditing. We also comply in all material respects with other Government guidance applicable to executive NDPBs.

1.2 Our Internal Audit Plan for the Information Commissioner's Office

Our proposed 2017-18 Internal Audit Plan has been prepared based upon:

- your latest risk register;
- our understanding of your key challenges and objectives; and
- discussions with management.

In taking this approach, and in compliance with PSIAS requirements, the Internal Audit Plan is developed to enable us to provide distinct assurance to the Management Board and the Information Commissioner (as Accounting Officer) as to the adequacy and effectiveness of the risk management activities and controls in each of the three areas of:

- risk management;
- governance; and
- internal control.

2 Internal Audit Plan 2017-18

2.1 Reporting outputs

Our Internal Audit Plan will deliver the following reporting outputs to management and the Audit Committee throughout the year:

- audit planning briefs;
- assignment reports;
- progress reports to the Audit Committee; and
- Internal Audit Annual Report.

Audit planning briefs

Every internal audit assignment will have audit planning brief that must be agreed with you before we begin any audit fieldwork. As well as capturing the background of the audit area, the scope of the review and the approach we will take, it also identifies key members of your staff who we will engage with and a timetable for fieldwork and reporting. It is prepared following detailed planning meeting(s) with your nominated client leads, and typically takes place six to eight weeks before our fieldwork begins. Each brief is subject to our usual quality assurance arrangements, i.e. is reviewed by the engagement manager and partner before it is issued to you for approval.

Assignment reports

We produce a separate assignment report for every review in the Plan. It has two core sections:

- an Executive Summary of the scope, key findings, best practice and our rating for the review area
- a schedule of our detailed findings, including our agreed audit recommendations and your management response.

We issue the assignment report in draft for your consideration and response within 15 days of completing our fieldwork. It is subject to our internal quality assurance review processes before it is issued in draft.

Progress reports to management and the Audit Committee

We issue a progress report to support to each meeting of the Audit Committee that shows the current status of each assignment in the Plan and highlights any emerging risks that may warrant a variation to the Plan.

Internal Audit Annual Report

Our Internal Audit Annual Report will contain our annual opinion on risk management, governance and internal control. It will summarise:

- the overall rating and level of recommendations for each audit assignment;
- how each review has informed the annual opinion we give, and the reasons behind any qualification we may give;
- progress made in addressing any significant findings; and
- our performance against agreed performance indicators.

2.2 Proposed Internal Audit Plan

We identify below the areas agreed for consideration in the Internal Audit Plan, which we will keep under review throughout the year.

Review	Scope	Audit Lead	Budget estimate 2017-18			
			Q1	Q2	Q3	Q4
Reviews for consideration						
Data Protection Law Reform follow up	The follow up the project review from 2016-17 and will include the follow up to the People Strategy review carried out by Internal Audit in 2016. It will establish that the findings have been actioned and that the project overall is on track to deliver the outcomes each workstream is required to deliver. Focus will be on the People Strategy and how the capacity and capability risks are being managed.	Paul Eckersley	0	10	0	0
Corporate Governance	Internal Audit has not reviewed the ICO corporate governance arrangements in the last four years. The review will cover how corporate governance arrangements have changed for 2017-18 (including risk management) and incorporated the changes to the organisation. The ICO has established a new senior leadership team and the Information Commissioner started in July 2016. The review will compare new governance and organisation structures to best practice.	Paul Eckersley	0	0	14	0
Fee Forecasting	Should the ICO establish a revised income through a new Registration Fees model and potentially other sources of income, the ICO may be able to plan more strategically and hence deliver more services (such as investigations, education programmes, audits). The audit will establish how the ICO established what the income should be from fees and incorporate the process to chase outstanding fee payment.	Paul Eckersley	0	0	8	0
IT Procurement	ICO will be involved in more procurement of IT products and services as the strategy is to take more responsibility for IT services. The review will establish the approach to procuring IT services and establish that the ICO will be able to go to market making use of existing government procurement frameworks where appropriate and ensue that those frameworks represent value for money.	Paul Eckersley	9	0	0	0
IT supplier Contract Management	The ICO currently has one main IT services contract with Northgate and a number of smaller or specialist suppliers. While there is formality over the Northgate contract management the level of formal management over the smaller value contacts may be insufficient. The review will establish whether sufficient controls are in place for smaller contracts.	Paul Eckersley	0	0	0	8
Follow Up	Review of the arrangements to capture and implement audit recommendations in a timely manner.	Paul Eckersley	0	0	0	3.5
	Sub-total by quarter		***9.0***	***10.0***	***22.0***	***11.5***
Planning, continued liaison, attendance at Audit Committee, annual reporting						
TOTAL						

Management has not deferred any of the areas considered.

2.3 Reviews to be considered for future audit plans

Review	Scope	Budget estimate Audit year 2018-19	Budget estimate Audit year 2019-20
Strategic / Regulatory			
GDPR implementation	The General Data Protection Regulation has been finalised and individual countries have until May 2018 to implement the regulation. The ICO has established a programme of work to deal with the impact of GDPR which was covered in the 2016-17 audit plan. This review is to confirm that the programme has met or is meeting its objectives.	8-10	
Financial controls			
Fee income changes/fees forecasting	Future work and organisational planning will become more reliant upon the ability of the ICO to forecast its income. The ICO has historically used to a budget model where expenditure could not exceed the budget. However, if the ICO was able to establish the expected income from Registration Fees, the ICO may be able to plan more strategically and hence deliver more services (such as investigations, education programmes and audits). The audit will establish how the ICO established what the income should be from fees and incorporate the process to chase outstanding fee payment.		7
Human Resources	Review of how staff management is delivered and covers staff planning, recruitment, performance management, employment contracts and payroll.		8
Operational controls			
Recruitment/performance management	Internal Audit reviewed recruitment, staff performance management in 2015-16, identified a number of areas of improvement, and this review is to follow up this review. The main focus of the review will be to establish that recruitment and staff performance is meeting the requirements of the ICO, especially as the detailed impact of changes to the ICO role (such as the implementation of GDPR) remains unknown.	8	
Facilities Management / Accommodation	The next lease break point for Wycliffe House will be 31 December 2021. The ICO will need to prepare its position two years in advance; ie during 2019/20		8-10
Health and Safety	The ICO has a legal requirement to ensure it provides a safe environment to work for its staff and visitors. The review will ensure that the organisation is monitoring the requirements of Health and Safety legislation as well as reviewing the risks associated with health and safety incident not being appropriately managed.		8-10

Review	Scope	Budget estimate	
		Audit year	
		2018-19	2019-20
IT controls			
IT service delivery (post contractual changes)	The contract with Northgate has a break point in 2017, and therefore it is a possibility that the replacement contract may expire in 2020 and planning for a replacement will need to take place in 2018. The review will focus on the planning for extension or replacement of the contract.	8-10	
Case management system replacement	The case management system is expected to be implemented within ICE, to replace CMEH. The expectation is that the development / implementation in 2017-18. The review will establish that the requirements of the ICO have been captured and that a project / project team is in place to implement the necessary changes.	8-10	
TOTAL		48-54	31-35

3 Previous Audit Plans and Resources

3.1 Previous Internal Audit plans / Audit Universe

The table below sets out the assurance provided over the last four years audits and potential review areas that have not been covered in that period:.

Review	13-14	14-15	15-16	16-17
Strategic / Regulatory				
Assurance mapping / sources of assurance	Management to consider			
Corporate Governance	Proposed for 2017-18			
Governance and decision making	x			
Integrated assurance		x		
Risk management and horizon scanning	x			
Operational				
Business and corporate planning		x		
Core operations (post-Eagle)			x	
Cryptographic Controls				x
Facilities Management / Accommodation	Proposed for 2019-20			
Fines recovery				x
Health & Safety	Management to consider			
Investigations				x
Payroll and pensions	x			
People Strategy				x
Policy and Procedures	Management to consider			
Social media	Management to consider			
Staff performance management			x	
Stakeholder engagement				x

Review	13-14	14-15	15-16	16-17
Financial				
Business and corporate planning		x		
Card payment controls in ICE	x			
Core financial controls			x	
Fraud prevention and monitoring	Management to consider relevance to ICO			
Staff recruitment			x	
IT				
IT Asset Management				x
IT contract management	x			
IT service management	x			
IT support		x		
Programme / Change				
Finance system – benefit realisation			x	
Finance system project assurance		x		
IT re-procurement lessons learnt	x			
GDPR project				x
Programme and Project management	Management to consider			
Total of plan (days)	**Redacted**			

3.2 Resources to deliver the Internal Audit Plan

Redacted to preserve confidentiality

A ICO risk register

We set out below the alignment of what the ICO sees as its key risks (the major risk groups) and the associated Internal Audit reviews.

Risk	Summary information – as per ICO risk register (January 2017)	Covered in 2017-18 Internal Audit Plan	Elements of risk within scope
1. Change – GDPR legislation	Amendments to UK legislation, needed because of GDPR, are too late to allow the ICO, as regulator, to adequately plan and prepare for implementation.	Yes	Data protection Law Reform – follow up Recruitment – new staff to prepare for new legislation
2. Change – un-prepared	The ICO is not prepared for change, either internal (new senior managers and organisational structure) or external (in particular implementation of the GDPR).	Yes	Management Governance GDPR – follow up Corporate Governance Recruitment – new staff to prepare for new legislation
3. Relevance	The ICO is seen as not being relevant to information rights issues of the day by its stakeholders (the public, media, government, elected representatives and organisations), and hence loses influence.	Yes	GDPR
4. Horizon scanning	The ICO does not identify key information rights trends and issues and is not successfully scanning the horizon, in consequence the ICO is not able to react as a credible regulator should; losing influence and reputation.	Yes	Management governance GDPR – follow up
5. Resources planning	The ICO is not planning and managing its resources (money, people or IT) as well as it could during a period of change and hence is not doing working as effectively as it should.	Yes	Management Governance Recruitment – new staff to prepare for new legislation Fee forecasting
6. DP income pre GDPR implementation	The ICO does not have enough income in 2017/18 to adequately prepare for GDPR implementation; either because of a fall off in notifications because of economic circumstances or to uncertainty for data controllers about the new funding regime coming into place by May 2018	Yes	Management Governance Fee forecasting
7. DP income post GDPR implementation	The ICO does not have enough income to adequately fund GDPR work once the current notification fee regime ends in May 2018.	Yes	Management Governance Fee forecasting

www.grant-thornton.co.uk